

REMARKS

Applicant requests reconsideration of the claim rejections in view of the arguments presented below.

It is noted that at section 4 of the Official Action, the Office indicates that the rejections under 35 USC §101 and 102 have been withdrawn. Further, it is noted that at sections 5 and 6, the Office asserts that applicant's arguments presented in the amendment filed on April 27, 2007 are not found persuasive.

For the reasons presented below, it is believed that pending claims 1-31 are distinguished over the art and that applicant's previous arguments and those contained herein support this conclusion.

Claim Rejections - 35 USC §103

At section 8, claims 1, 12-19, 25, 26 and 28-31 are rejected under 35 USC §103(a) as being unpatentable over Applicant's Admitted Prior Art (APA) in view of Stallings (William Stallings, "Cryptography and network security", second edition, 1998, ISBN: 0138690170).

Independent Claims 1, 25, 26, 28, 30 and 31

At sections 5, 6, 8 and 9 of the final Official Action, the Office asserts that claim 1 is unpatentable in view of the APA¹ in combination with Stallings. The Office states at section 6 that the APA discloses essentially the same elements as the claim language with the only difference being that the APA does not disclose that an entity generating a set of secrets (first part and a second part of a predetermined master key) used in a secure transaction (e.g., authorization) is not the same as one of the parties participating in the transaction. However, the Office states that separating a party generating a set of secrets from parties that utilize a secret from the set of secrets in secure transactions is disclosed in Stallings. These assertions are believed to be incorrect for the following reasons:

¹ It is noted that the APA specifically identifies MacKenzie, et al. "Networked cryptographic devices resilient to capture". The subject matter of MacKenzie is discussed in Section 8 of the final Official Action.

1) In contrast to the position taken by the Office with respect to claim 1, MacKenzie does not disclose transmitting a partial secret key from a device to a server with which the device intends to cooperate with for accessing resources by applying partial secret key operations. MacKenzie does not disclose that a device transmits a first part of a secret key to a server and a second part of the secret key to another device, which is to be enabled to cooperate with the server for accessing resources by applying partial secret key operations. According to claim 1, two parts of a secret key are used by two parties in cooperation, where both parties are different from the owner of the secret key (the master device).

2) Stallings only deals with the distribution of public keys between devices via a server. The Office completely neglects the nature of the fact that these are public keys disclosed in Stallings. As is well-known to those skilled in the art, a public key is not a secret key. A public key can thus not be considered to be one secret of a set of secrets. The secret keys dealt with in Stallings are only the private keys, which are never transmitted, neither entirely nor partially. Authorization to access resources is only provided by the private keys. The public keys can be used by anyone for encryption purposes, but an encryption does not provide any access to resources as is well-known in the art. There is clearly a significant difference between distributing non-secret keys (public keys) to any requesting device as taught by Stallings as compared to forwarding a part of the secret key to a selected trusted device as is disclosed and claimed in the present invention in claim 1. Thus, a person of ordinary skill in the art would have no incentive to apply the teachings of Stallings to those of MacKenzie.

3) In Stallings, there is no party generating a set of secrets, but rather only a party generating a private key for its own use and an associated public key for distribution via a server. Thus, it is not possible that Stallings discloses separating a party generating a set of secrets from parties that utilize a secret from the set of secrets in a secure transaction. In Stallings, the only and entire secret key always stays at the party generating the secret key. Thus, there is not even any set of keys that is provided to two parties that are different from the party that generated the keys, much less a set of secret keys and further much less than two parts of the same master key as required by claim 1.

For all of the foregoing reasons, it is therefore respectfully submitted that claim 1 is not unpatentable over the APA in view of Stallings.

For similar reasons, independent claims 25, 26, 28, 30 and 31 are also distinguished over the APA in view of Stallings.

Dependent Claim 2 and Independent Claims 27 and 29

Claims 2, 27 and 29 relate to a chained delegation of an authorization. At section 14, the Office considers a chain delegation to be simply a recursive repetition of the teachings of MacKenzie in view of Stallings. A recursive repetition of splitting a secret key to partial secret keys is argued to be known from MacKenzie and Reiter ("Delegation of Cryptographic Servers For Capture-Resilient Devices", Chapter 3.4). Applicant respectfully disagrees with this argument.

More specifically, MacKenzie and Reiter only suggest that available shares d_1 and d_2 are used for generating additional shares d'_1 and d'_2 such that $d'_1 + d'_2 = d_1 + d_2$. This arrangement enables the same device to cooperate with different servers. When applied to MacKenzie, this approach in MacKenzie and Reiter at most would teach a person of ordinary skill in the art that a device could generate a plurality of equivalent sets of partial keys for the same available secret key. Such is not the same as enabling a chained delegation, since it is always the same device that has to generate a set of partial keys. The reason is that according to MacKenzie and Reiter, the entire information is always required for generating a new set of shares: It is defined that d'_2 is constructed as $d'_2 = (d_1 - d_{11}) + (d_2 - d_{21})$; the construction thus requires knowledge of both original shares d_1 and d_2 .

However, this arrangement is not the teaching of claims 2, 27 and 29. In these claims,² a delegatee receives a partial key d_1 , splits only this partial key d_1 into parts d_{11} and d'_{21} of partial key d_1 . In the approach of the present application as set forth in claims 2, 27 and 29, the delegatee is thus not required to have any knowledge about partial key d_2 . One part d_{11} of partial key d_1 is then transmitted to a sub-delegatee and the other part d'_{21} of partial key d_1 is transmitted to the server. The server is thus

² See exemplifying embodiment shown in Figure 2 and the accompanying description in the specification, including page 17, line 32 through page 20, line 11.

required to be able to combine an equally available partial key d_2 with the part d'_{21} of partial key d_1 to obtain a new partial key d_{21} before being able to apply its part of a secret key operation in cooperation with the sub-delegatee using the new partial key d_{11} . Thus, $d_{11} + d'_{21} + d_2 = d_1 + d_2$.

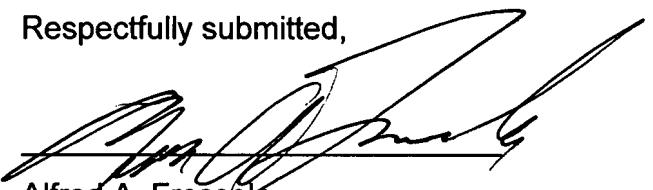
It is therefore respectfully submitted that dependent claim 2 is further distinguished over the APA in view of Stallings further in view of MacKenzie and Reiter and that independent claims 27 and 29 are similarly distinguished over the cited art.

In view of the foregoing, since each of the independent claims is believed to be distinguished over the cited art, it is respectfully submitted that all of the dependent claims are further distinguished over the cited art.

It is therefore respectfully requested that reconsideration of the rejection of claims 1-31 be made and that the application proceed to allowance.

The undersigned respectfully submits that no fee is due for filing this Request for Reconsideration. The Commissioner is hereby authorized to charge to deposit account 23-0442 any fee deficiency required to submit this paper.

Respectfully submitted,



Alfred A. Fressola
Attorney for Applicant
Reg. No. 27,550

Dated: September 28, 2007

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955